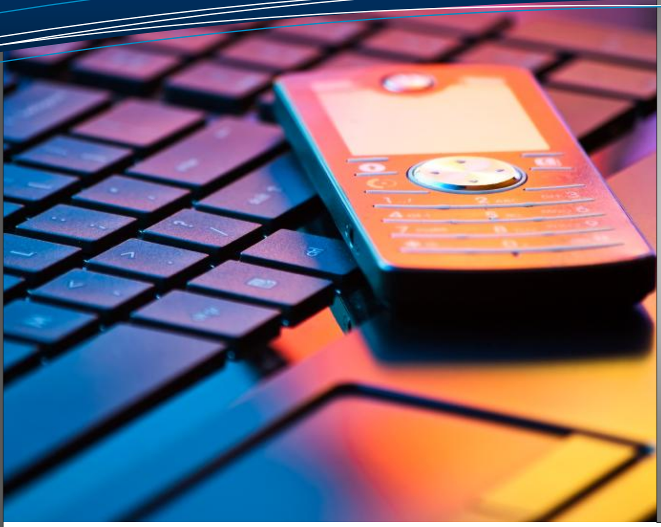
July

2011

MONTHLY
Cyber Security
Newsletter

Security Tips



Mississippi Department of Information Technology Services

Division of Information Security

What's new this month?

This month we will discuss the risks involved with mobile devices as well as a deeper look inside virtualization.

Securing Mobile Devices – Big Things Come In Small Packages!

Mobile computing devices include mobile phones, IP phones, pagers, BlackBerry devices, iPhones, smart phones, and portable storage devices, such as USB drives. Some of these devices are multifunctional and may be used for voice calls, text messages, email, Internet access, and may allow access to computers and/or networks. Some also include Near Field Communication (NFC) capabilities, which allows the user to perform activities such as debit/credit card transactions or utilizing the device as a car and/or house key. Mobile computing devices have become indispensable tools for today's highly mobile society. Small and relatively inexpensive, these multifunction devices are becoming as powerful as desktop or laptop computers. While increased productivity is a positive feature for any organization, the risks associated with mobile devices can be significant and include issues stemming from human factors to technological issues.

The Risky Business of Mobility!

A significant amount of personal, private and/or sensitive information may be stored or accessed via mobile devices. The portable nature of mobile devices makes it more difficult to implement physical controls. Additionally, the fact that some employees are increasingly using their personal mobile devices for business purposes have resulted in heightened risks. Ironically, many of the risks associated with mobile devices exist because of their biggest benefit: portability. Many of these devices can store vast amounts of data, making them vulnerable to unauthorized access to the information from either interception of data in transit or theft or loss of a device. In addition to data loss, mobile computing devices carry the risk of introducing malware. Certain types of malware can infect the devices or can be used as a platform for malicious activity. Devices with onboard microphones and cameras are also vulnerable to unintended activity through publicly available tools, possibly resulting in eavesdropping or tracing the device's location. Cellular and Voice-over IP (VoIP) technologies also have vulnerabilities that can be easily exploited, resulting in intercepted calls.

What Can Be Done to Secure Mobile Computing Devices?

The protection of mobile devices must be a primary task for organizations. The following steps can help you protect your data and your mobile computing device:

- Organizations should have a policy to address the storage of information on mobile devices, including the use of personal devices for business purposes.
- Keep your mobile device physically secure. Millions of mobile devices are lost each year.
- Control what data is stored on the device. Do not store unnecessary or sensitive information.
- Use a secure password or PIN to access your device. If the device is used for business purposes, you should follow the password policy issued by your organization.
- Disable features and services that are not needed (Bluetooth, WiFi, GPS, etc). If the Bluetooth functionality is used, be sure to change the default password.
- Enable storage encryption. This will help protect the data stored on your device in the event it is lost or stolen, assuming you have it password protected.
- If available, consider installing anti-virus software for your mobile device. This may prevent or detect/quarantine malware specific to mobile devices.
- Keep all system and application software patched and up-to-date. Many manufacturers frequently provide updates to address known vulnerabilities.
- Download applications only from vendor-authorized sites. Sites offering “free games” or “ring tones” are sources for distributing malware. If used for work, follow your organization’s policy on downloading software.
- Do not open attachments from untrusted sources. Similar to the risk when using your desktop, you risk being exposed to malware when opening unexpected attachments.
- Do not follow links to untrusted sources, especially from unsolicited email or text messages. As with your desktop, you risk being infected with malware.
- If your device is lost, report it immediately to your carrier or organization. Some devices allow the data to be erased remotely.
- Before disposing the device be sure to wipe all data from it. If used for work, follow your organization’s policy for disposing of computer equipment.

Resources For More Information:

National Cyber Alert System - Cyber Security Tip ST06-007, Defending Cell Phones and PDAs Against Attack
us-cert.gov/cas/tips/ST06-007.html

NIST Special Publication 800-124, Guidelines on Cell Phone and PDA Security
csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

FTC Consumer Alert – The 411 on Disposing of Your Old Cell Phone
ftc.gov/bcp/edu/pubs/consumer/alerts/alt044.shtm

For more monthly cyber security newsletter tips, visit: www.msisac.org/awareness/news/

this newsletter is brought to you by…

www.msisac.org

www.its.ms.gov/services_security.shtml

Virtual Machines – Real Security

Jimmy Webster

Virtualization, as we understand it today in Information Technology (IT), is the creation of a virtual instance of hardware, operating systems, storage, or network resources by using software to exponentially increase the cost effective use of those physical resources. For the purposes of this particular article, we are specifically looking at the security issues involving the virtualization of multiple operating systems on a single machine and the challenges that presents. Virtualization in today's enterprise IT environment includes the use of autonomic computing, which is defined as self-managing characteristics of distributed computing resources where the virtual systems adapt to unpredictable changes, all without direct involvement of IT staff or users. This type of intelligence, automation, flexibility, and efficiency demands we pay close attention to the details when defining the agency virtual environment and the responsibilities that go along with supporting the virtual machine (VM) environment.

Because virtualization platforms are built on software, and software inherently has imperfections, it stands to reason that virtualization platforms will also suffer from imperfections that will create vulnerabilities in those platforms. Obviously, the major manufacturers of these platforms will seek to identify these issues and address them with minimal impact to their customers, but the customer will need to understand the security implications and take the necessary steps to protect their data and systems. Some of the primary areas where security professionals should focus their attention include:

- **Management and Monitoring –** One of the most common issues with the deployment of VMs is the potential for IT or security managers to lose control of them because the responsibility for managing VMs is not always well defined. Once the physical environment and infrastructure is setup, it is simple and fast to deploy an instance. The ability to turn up instances in a moment's notice, for a demo or test of an application, makes us much more responsive and agile. However, ease of deployment can create a lack of properly infused security controls, which are necessary to ensure that the environment is being adequately managed, tracked, and documented. It is important to have someone charged with the responsibility of managing and securing all the virtualized assets in the agency.

- **Patch Management –** Though patch management can be a labor intensive function, it is still imperative that sound patch management practices be implemented for the virtualized environment. The practice of patch management in the virtualized environment is made more difficult because virtual machines tend to be launched from server images that may have been created, configured and patched weeks or months before, but that simply means that the patch management processes and procedures need to be clearly and concisely documented and tracked. These practices should include maintaining the latest service packs for both guests and hosts, alleviating any unnecessary applications that have a history of vulnerabilities, and applying the latest security rollup patches supplied by the virtual software vendors.

- **Configuration Management** – Using “best practice” configuration guidelines including setting file permissions, controlling users and groups, setting up logging and time synchronization, and turning off services you don’t need, can have a significant impact on your security posture. The technology is new and there is still a lot to learn, but by defining specific policies and configuration guidelines, creating procedures to implement the policies, and then using them to properly configure and lock down systems, you can significantly reduce your exposure.

- **Communications** - Securing communications between the host system and desktops or a management infrastructure component is essential to prevent eavesdropping, data leakage, and Man-in-the-Middle attacks. Most of the well-known platforms today support SSH, SSL and IPSec for any communications that are required, and one or more of these should be enabled.

This complex integrated virtual environment introduces new opportunities for exposure and vulnerability that must be considered when implementing, especially at the rate of growth in deployment of VMs. According to Gartner, virtualization is becoming a mainstream platform where 23% of installed applications are running in a VM today, some 48% of installed applications will run on a VM by 2012. This is the future and we had better be prepared for it, or it will simply run us over. As the author Robert C. Gallagher once said, “Change is inevitable … except from a vending machine”.

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization’s end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization’s overall cyber security posture. This is especially critical if employees access their work network from their home computer. ***Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.***